

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**RECEIVED
CENTRAL FAX CENTER****DEC 20 2004**

In re application of	:	December 20, 2004
Mark E. Peters	:	IBM Corporation
Ser. No. 09/240,265	:	Dept.T81/Bldg. 503
Filed January 29, 1999	:	P.O. Box 12195
For: Extension of X.509 Certificates to	:	Res. Tri. Park, NC 27709
Simultaneously Support Multiple	:	Art Unit: 2137
Cryptographic Algorithms	:	Examiner: D. J. Meislahn

APPEAL BRIEF

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Sir:

The following remarks in the Appeal for the above identified Application are respectfully submitted:

REAL PARTY IN INTEREST

This Application has been assigned to the International Business Machines Corporation.

RELATED APPEALS AND INTERFERENCES

Applicants know of no other Appeals or Interferences which will directly affect or

Serial No. 09/240,265

1

be directly affected by or having a bearing on the Boards decision in the pending Appeal.

STATUS OF CLAIMS

The Application was originally filed with Claims 1 - 3. Claims 4 - 6 were added in the Amendment filed on February 12, 2003. Claims 5 and 6 were amended and Claims 7 - 9 were added in the Amendment filed on July 15, 2003. Claims 1 and 7 were amended and Claims 10 - 12 were added in the Amendment dated February 9, 2004. Accordingly, Claims 1 - 12 remain pending, and these are the claims which are the subject of this Appeal. A copy of the appealed claims, Claims 1 - 12, are contained in the attached Appendix.

STATUS OF AMENDMENTS

Applicants last filed an Amendment on February 9, 2004, which was entered. No further amendments were made to the Application.

SUMMARY OF THE INVENTION

The present invention discloses an extended X.509 certificate capable of supporting more than one cryptographic algorithm. The certificate comprises a signature algorithm and a signature for all authenticated attributes using a first cryptographic algorithm, and alternative public key extension for identifying at least one alternative cryptographic algorithm and providing its associated public key, and an alternative signature extension for containing a signature for the alternative cryptographic algorithm.

STATEMENT OF ISSUES PRESENTED

Applicants present for review the final rejection of Claims 1 through 12 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,923,756 to Shambroom and passages from the Schneier book "Applied Cryptography" in view of U.S. Patent No. 6,157,721 to Shear et al. Applicants also present for review the final rejection of Claims 1 - 3 under 35 U.S.C. Section 101 for being directed to non-statutory subject matter.

GROUPING OF THE CLAIMS

Independent Claim 1 stands or falls alone.

Dependent Claims 2 and 3 stand or fall with Claim 1.

Independent Claims 4, 7 and 10 stand or fall together.

Dependent Claims 5, 6, 8, 9, 11 and 12 stand or fall with Claims 4, 7 and 10.

ARGUMENT

Applicant traverses the rejections below.

A. Differences Between the Claimed Invention and the Cited Art

1. Independent Claim 1

Claims 1 through 12 were rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,923,756 to Shambroom and passages from the Schneier book "Applied Cryptography" in view of U.S. Patent No. 6,157,721 to Shear et al.

Shambroom discloses a technique for enhancing the security of a message sent through a network server from a client computer to a destination server. A secure connection for receiving and transmitting data is established between the client and the server. Using client identification information and a secure authentication protocol, the server obtains client-authentication information from a validation center. This information is transmitted to the client and erased from the server.

Relative to Claim 1, the Office Action identifies a passage from Shambroom as disclosing "a certificate that supports one or more cryptographic algorithms" and that "the certificate can resemble an X.509 certificate," citing Column 10, lines 32-35

More specifically, Shambroom states that "web server 720 responds with a certificate to web browser 620. This certificate contains the network server's public key and a list of one or more cryptographic algorithms that the network server supports..." (Column 10, lines 30-34).

The key here is that the Shambroom certificate contains a list of one or more cryptographic algorithms that the **network server** supports. The Shambroom certificate does not actually use or employ multiple cryptographic algorithms to protect the data therein. The Shambroom data appears to be the list of algorithms. The certificate in Claim 1 does **not** contain a list of cryptographic algorithms that a network server supports. The claimed certificate utilizes and uses more than one cryptographic algorithm itself to protect the data it includes.

Further, the network server's public key appears to be used by the web browser to log onto or communicate with the web server 720, which is part of the network server 700, and not to protect the data in the certificate. In other words, the Shambroom certificate is used to transfer data, including the list of cryptographic algorithms that the network server supports and the public key for the network server, to the web browser.

No such scheme is contemplated by the present invention.

The Office Action goes on to state that the "list of algorithms disclosed in Shambroom also anticipates an extension for identifying at least one alternative algorithm." This statement is not supported by Shambroom. Shambroom does not mention certificate extensions. The Shambroom list is not a certificate extension. There is no mention that the list takes the form of a certificate extension. Rather, as discussed above, the list is data which is relevant to which algorithms the network server supports. They have nothing to do with protecting the information in the certificate, as per the claimed subject matter.

Claim 1 recites that the X.509 certificate comprises "a signature algorithm and signature for all authenticated attributes using a first cryptographic algorithm;" as well as "an alternative public key extension for identifying at least one alternative cryptographic algorithm and providing its associated public key; and an alternative signature extension for containing a signature for the alternative cryptographic algorithm." This is not the same thing as a list of cryptographic algorithms that a network server supports as per Shambroom, and such a list included in a certificate does not teach, suggest or disclose the subject matter of Claim 1. Shambroom does not teach that its certificate protects its data using more than one cryptographic algorithm. The Shambroom list appears to be data included in the certificate, not multiple cryptographic algorithms employed by the certificate to protect its data, as per Claim 1.

Schneier appears to describe a standard X.509 certificate which employs a single cryptographic algorithm.

Including a list of cryptographic algorithms as data in a certificate does not teach, suggest or disclose using multiple algorithms to protect the data in the certificate. There is no reason to combine Shambroom's list of cryptographic algorithms contained in a certificate (which indicate which algorithms a server supports) with the standard

X.509 certificate, such as that of Schneier, which actually uses a single algorithm to protect data contained therein.

The final Office Action also uses the Shear reference in combination with Shambroom and Schneier to reject Claim 1. Shear is directed to security for load modules. In the Abstract, Shear states that the use of "several dissimilar digital signature algorithms may be used to reduce vulnerability from algorithm compromise, and subsets of multiple digital signatures may be used to reduce the scope of any specific compromise."

However, Shear does not suggest, teach or disclose creating extensions to a certificate. The Office Action argues that it would be obvious to put multiple signatures formed with different algorithms into Shambroom's certificate based on the teachings of Shear.

Applicant has never argued that the present invention claims the concept of using more than one algorithm for the purpose of security. Rather, Applicant has figured out how to make such a multiple algorithm system work with respect to certificates. This involves the use of extensions. And none of the references teaches this or mentions the use of extensions in such a manner. None of Shambroom, Shear and Schneier discusses the use of extensions to enable the certificate to support an alternative cryptographic algorithm, as per the second and third elements of Claim 1.

In a number of the Office Actions, the Examiner has noted that "one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references." On some level, this may be true. However, if an applicant can show that a given reference does not in fact teach, suggest or disclose those portions of the claims that the reference is utilized in a rejection to teach, suggest or disclose, then the combination is improper and the obviousness rejection cannot stand. If individual references may not be attacked, then a reference directed to mousetraps

could be combined with a reference directed to a semiconductor in order to render claims directed to bioengineered corn obvious with neither the semiconductor reference nor the mousetrap reference being 'attackable' individually. Certainly, each reference may be 'attacked' for not teaching, suggesting or disclosing what they are alleged to teach, suggest or show, thus rendering the scope of the combination incomplete relative to the claimed subject matter.

In one of the Office Actions it is argued that "the bits in Shambroom that identify the cryptographic algorithms, which are additional information, read on an extension." What this discussion shows is that the rejections over the art are taking little bits and pieces out of the various cited references and combining them in a way not contemplated by the references as a collection and without an teaching to combine the references in the manner combined. Are "bits" from Shambroom to which the Office Action is referring to the "list" of algorithms. An extension is a well-defined term of art in the certificate art. The addition of bits to a list of algorithms does not teach, suggest or disclose adding an extension to a certificate.

In the Office Action dated April 15, 2003, it was argued in numbered paragraph 3 that the fact that the "present invention does not transfer data that includes a list of cryptographic algorithms" does not matter, because "applicant has recognized another advantage which would flow naturally from following the suggestion of the prior art..." Applicant has made no such recognition. As discussed above, a list of algorithms does not anticipate an extension for identifying at least one alternative algorithm. The argument in paragraph 3 is not supported by Shambroom. Shambroom does not mention certificate extensions. The Shambroom list is not a certificate extension. There is no mention that the list takes the form of a certificate extension. Rather, as discussed above, the list is data which is relevant to which algorithms the network server supports. They have nothing to do with protecting the information in the certificate, as per the claimed subject matter.

In numbered paragraph six of the April 15, 2003 Office Action, the Office Action states that the combination of references is proper because "Shear et al, while specifically directed to load modules, executables, and other data elements teaches multiple signatures created with dissimilar algorithms in a broadly applicable fashion, and thus the combination is proper." As noted above, the most pertinent passage of Shear states, in the Abstract, that the use of "several dissimilar digital signature algorithms may be used to reduce vulnerability from algorithm compromise, and subsets of multiple digital signatures may be used to reduce the scope of any specific compromise." Shear is directed to security for load modules. There is nothing in the art that suggests the desirability to combine the references. Shear is directed to load modules and executables, not certificates. The ability to enable a certificate to support more than one cryptographic algorithm is an entirely different problem.

In numbered paragraph seven of the Office Action of April 15, 2003, the Office Action erroneously states that "applicant agrees that the claims recite data." What Applicant stated is that the claims recite functional structure for data, much like Shear. It is interesting that the Office Action goes on to state that Shear claims physical objects. If this is the case, then Shear clearly cannot be combined with the other references, as the other references are not directed to physical objects. However, Applicant believes Shear to be directed to code, and the barrier, arrangement and load module of Shear's claim 14 are certainly not a physical barrier, a physical arrangement and a physical load module, but functional structures for data. Physical names have been provided to these structural elements which are purely code based.

Accordingly, Applicant submits that Claim 1 patentably distinguishes over the combination of Shambroom, Shear and Schneler. Applicant respectfully request that the Board overturn this rejection of Claim 1

2. Independent Claims 4, 7 and 10

Independent Claims 4, 7 and 10 were rejected for the same reasons as was Independent Claim 1. Accordingly, it follows that Claims 4, 7 and 10 distinguish over the cited art, and respectfully request that the Board overturn these rejections.

3. Dependent Claims 2, 3, 5, 6, 8, 9, 11 and 12

Since the independent claims have been shown to patentably distinguish over the cited art, it follows that the dependent claims also distinguish therefrom. Accordingly, Applicant respectfully requests that the Board overturn the rejection of Claim 2, 3, 5, 6, 8, 9, 11 and 12 over the art.

B. Improper Combination of References

Additionally, the Examiner has failed to provide a convincing line of reasoning for combining the teachings and structure of Shambroom with the teachings and structure of Schneier and the teachings and structure of Shear so as to arrive at the present claimed invention. Under 35 U.S.C. Section 103, when the Examiner has relied on the teachings of several references, the test is whether or not the references viewed individually and collectively would have suggested the claimed invention to the person possessing ordinary skill in the art. See *In re Kaslow*, 707 F.2d 1366, 217 USPQ 1989 (Fed. Cir. 1983). It is to be noted, however, that citing references which merely indicate that isolated elements and/or features recited in the claims are known is not a sufficient basis for concluding that a combination of claimed elements would have been obvious. That is to say, there should be something in the prior art or a convincing line of reasoning suggesting the desirability of combining the references in such a manner as to arrive at the claimed invention. See *In re Deminski*, 796 F.2d 436, 230 USPQ 313 (Fed. Cir. 1986).

Applicant submits that there is no teaching in the reference or a convincing line

of reasoning provided by the Examiner to combine the teachings of Shambroom, Shear and Schneier so as to arrive at the present claimed invention. Shambroom discloses a certificate that contains a list of one or more cryptographic algorithms that a **network server** support. Schneier describes a standard X.509 certificate which employs a single cryptographic algorithm. Shear is directed to security for load modules which uses several dissimilar digital signature algorithms. No reason is provided for combining a certificate which carries a list of algorithms (Shambroom) with a standard X.509 certificate (Schneier) with the concept that multiple dissimilar digital signature algorithms may be used for security for load modules. How and why anyone would combine these references so as to arrive at the present claimed invention is entirely unclear. Certainly, nothing is provided in the references that would suggest combining these references. No appropriate line of reasoning is provided for combining these references. Accordingly, Applicant submits that the combination of references is inappropriate and improper and respectfully submit that this is a further reason to overturn the rejection that stands alone from the reasons discussed above relative to the content of the references.

Accordingly, Applicant submits that Claims 1-12 further distinguish over the cited art, and respectfully request that the Board overturn the rejection over the art for this reason as well.

C. Traversal of the Rejection under 35 U.S.C. Section 101

Claims 1 - 3 were rejected under 35 U.S.C. Section 101 for being directed to non-statutory subject matter. The rejection states that the claims "claim data."

Applicant submits that the claims are statutory. The claims recite a functional structure for data stored on a computer readable media. The claims do not recite sales data or a list of addresses. For example, in the Shear patent cited by the Examiner, Claims 14 and 34 recite a security structure. The barrier, arrangement and load

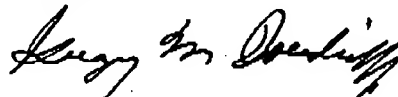
module of Shear's claim 14 are certainly not a physical barrier, a physical arrangement and a physical load module, but functional structures for data. This claim format is well accepted by the United States Patent and Trademark Office as being appropriate. The Office Actions do not describe in any detail why the claims of the present invention are unpatentable while the claims of Shear are patentable. The Office Actions have no detailed discussion as to why the claims are non-statutory. Since issued claims exist under the format alleged to be non-statutory in the final Office Action and no detailed explanation has been provided as to why the present claims are non-statutory while the issued claims are statutory, Applicant submits that this rejection is erroneous, and that Claims 1-3 are statutory. It also appears to follow that the USPTO is estopped from taking a different position relative to the present claims given its prior position on the same claim format without the benefit of any intervening statute or case law.

Accordingly, Applicant submits that Claims 1-3 are statutory, and respectfully requests that the Board overturn the rejection

SUMMARY

Applicant respectfully submits that the final rejections of the claims under 35 U.S.C. Sections 103(a) and 101 are improper and erroneous. Applicant respectfully urges the Board of Patent Appeals to reverse all grounds of the final rejection relative to the claims.

Respectfully submitted,



Gregory M. Doudnikoff
Attorney for Applicant
Reg. No. 32,847

2004-12-20 15:52

919-254-4330

919-254-4330 >> USPTO

P 22/55

GMD:ssc

Docket No: CR9-98-095

PHONE: 919-254-1288

FAX: 919-254-4330

Serial No. 09/240,265

12

APPENDIX

1. An X.509 certificate stored on computer readable medium, said certificate capable of supporting more than one cryptographic algorithm, comprising:

a signature algorithm and signature for all authenticated attributes using a first cryptographic algorithm;

an alternative public key extension for identifying at least one alternative cryptographic algorithm and providing its associated public key; and

an alternative signature extension for containing a signature for the alternative cryptographic algorithm.

2. An X.509 certificate according to Claim 1, wherein the first cryptographic algorithm is RSA and the alternative cryptographic algorithm is elliptic curve.

3. An X.509 certificate according to Claim 1, wherein the certificate can be verified by either the signature for the first cryptographic algorithm or the signature for the alternative signature algorithm.

4. A method for enabling an X.509 certificate to support more than one cryptographic algorithm, said method comprising the steps of:

providing the X.509 certificate with a signature algorithm and signature for all authenticated attributes using a first cryptographic algorithm;

providing the X.509 certificate with an alternative public key extension for identifying at least one alternative cryptographic algorithm and providing its associated public key; and

providing the X.509 certificate with an alternative signature extension which contains a signature for the alternative cryptographic algorithm.

5. A method for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 4, wherein the first cryptographic algorithm is RSA and the alternative cryptographic algorithm is elliptic curve.

6. A method for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 4, wherein the certificate can be verified by either the signature for the first cryptographic algorithm or the signature for the alternative signature algorithm.

7. Computer readable code stored on computer readable media for enabling an X.509 certificate to support more than one cryptographic algorithm, said computer readable code comprising:

first subprocesses for providing the X.509 certificate with a signature algorithm and signature for all authenticated attributes using a first cryptographic algorithm;

second subprocesses for providing the X.509 certificate with an alternative public key extension for identifying at least one alternative cryptographic algorithm and providing its associated public key; and

third subprocesses for providing the X.509 certificate with an alternative signature extension which contains a signature for the alternative cryptographic algorithm.

8. Computer readable code for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 7, wherein the first cryptographic algorithm is RSA and the alternative cryptographic algorithm is elliptic curve.

9. Computer readable code for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 7, wherein the certificate can be verified by either the signature for the first cryptographic algorithm or the signature for the alternative signature algorithm.

10. In a computing environment, a system for enabling an X.509 certificate to support more than one cryptographic algorithm, said system comprising:

means for providing the X.509 certificate with a signature algorithm and signature for all authenticated attributes using a first cryptographic algorithm;

means for providing the X.509 certificate with an alternative public key extension for identifying at least one alternative cryptographic algorithm and providing its associated public key; and

means for providing the X.509 certificate with an alternative signature extension which contains a signature for the alternative cryptographic algorithm.

11. A system for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 10, wherein the first cryptographic algorithm is RSA and the alternative cryptographic algorithm is elliptic curve.

12. A system for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 10, wherein the certificate can be verified by either the signature for the first cryptographic algorithm or the signature for the alternative signature algorithm.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**RECEIVED
CENTRAL FAX CENTER
DEC 20 2004**

In re application of	:	December 20, 2004
Mark E. Peters	:	IBM Corporation
Ser. No. 09/240,265	:	Dept.T81/Bldg. 503
Filed January 29, 1999	:	P.O. Box 12195
For: Extension of X.509 Certificates to	:	Res. Tri. Park, NC 27709
Simultaneously Support Multiple	:	Art Unit: 2137
Cryptographic Algorithms	:	Examiner: D. J. Meislahn

APPEAL BRIEF

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Sir:

The following remarks in the Appeal for the above identified Application are respectfully submitted:

REAL PARTY IN INTEREST

This Application has been assigned to the International Business Machines Corporation.

RELATED APPEALS AND INTERFERENCES

Applicants know of no other Appeals or Interferences which will directly affect or

Serial No. 09/240,265

1

be directly affected by or having a bearing on the Boards decision in the pending Appeal.

STATUS OF CLAIMS

The Application was originally filed with Claims 1 - 3. Claims 4 - 6 were added in the Amendment filed on February 12, 2003. Claims 5 and 6 were amended and Claims 7 - 9 were added in the Amendment filed on July 15, 2003. Claims 1 and 7 were amended and Claims 10 - 12 were added in the Amendment dated February 9, 2004. Accordingly, Claims 1 - 12 remain pending, and these are the claims which are the subject of this Appeal. A copy of the appealed claims, Claims 1 - 12, are contained in the attached Appendix.

STATUS OF AMENDMENTS

Applicants last filed an Amendment on February 9, 2004, which was entered. No further amendments were made to the Application.

SUMMARY OF THE INVENTION

The present invention discloses an extended X.509 certificate capable of supporting more than one cryptographic algorithm. The certificate comprises a signature algorithm and a signature for all authenticated attributes using a first cryptographic algorithm, and alternative public key extension for identifying at least one alternative cryptographic algorithm and providing its associated public key, and an alternative signature extension for containing a signature for the alternative cryptographic algorithm.

STATEMENT OF ISSUES PRESENTED

Applicants present for review the final rejection of Claims 1 through 12 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,923,756 to Shambroom and passages from the Schneier book "Applied Cryptography" in view of U.S. Patent No. 6,157,721 to Shear et al. Applicants also present for review the final rejection of Claims 1 - 3 under 35 U.S.C. Section 101 for being directed to non-statutory subject matter.

GROUPING OF THE CLAIMS

Independent Claim 1 stands or falls alone.

Dependent Claims 2 and 3 stand or fall with Claim 1.

Independent Claims 4, 7 and 10 stand or fall together.

Dependent Claims 5, 6, 8, 9, 11 and 12 stand or fall with Claims 4, 7 and 10.

ARGUMENT

Applicant traverses the rejections below.

A. Differences Between the Claimed Invention and the Cited Art

1. Independent Claim 1

Claims 1 through 12 were rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,923,756 to Shambroom and passages from the Schneier book "Applied Cryptography" in view of U.S. Patent No. 6,157,721 to Shear et al.

Shambroom discloses a technique for enhancing the security of a message sent through a network server from a client computer to a destination server. A secure connection for receiving and transmitting data is established between the client and the server. Using client identification information and a secure authentication protocol, the server obtains client-authentication information from a validation center. This information is transmitted to the client and erased from the server.

Relative to Claim 1, the Office Action identifies a passage from Shambroom as disclosing "a certificate that supports one or more cryptographic algorithms" and that "the certificate can resemble an X.509 certificate," citing Column 10, lines 32-35

More specifically, Shambroom states that "web server 720 responds with a certificate to web browser 620. This certificate contains the network server's public key and a list of one or more cryptographic algorithms that the network server supports..." (Column 10, lines 30-34).

The key here is that the Shambroom certificate contains a list of one or more cryptographic algorithms that the network server supports. The Shambroom certificate does not actually use or employ multiple cryptographic algorithms to protect the data therein. The Shambroom data appears to be the list of algorithms. The certificate in Claim 1 does not contain a list of cryptographic algorithms that a network server supports. The claimed certificate utilizes and uses more than one cryptographic algorithm itself to protect the data it includes.

Further, the network server's public key appears to be used by the web browser to log onto or communicate with the web server 720, which is part of the network server 700, and not to protect the data in the certificate. In other words, the Shambroom certificate is used to transfer data, including the list of cryptographic algorithms that the network server supports and the public key for the network server, to the web browser.

No such scheme is contemplated by the present invention.

The Office Action goes on to state that the "list of algorithms disclosed in Shambroom also anticipates an extension for identifying at least one alternative algorithm." This statement is not supported by Shambroom. Shambroom does not mention certificate extensions. The Shambroom list is not a certificate extension. There is no mention that the list takes the form of a certificate extension. Rather, as discussed above, the list is data which is relevant to which algorithms the network server supports. They have nothing to do with protecting the information in the certificate, as per the claimed subject matter.

Claim 1 recites that the X.509 certificate comprises "a signature algorithm and signature for all authenticated attributes using a first cryptographic algorithm;" as well as "an alternative public key extension for identifying at least one alternative cryptographic algorithm and providing its associated public key; and an alternative signature extension for containing a signature for the alternative cryptographic algorithm." This is not the same thing as a list of cryptographic algorithms that a network server supports as per Shambroom, and such a list included in a certificate does not teach, suggest or disclose the subject matter of Claim 1. Shambroom does not teach that its certificate protects its data using more than one cryptographic algorithm. The Shambroom list appears to be data included in the certificate, not multiple cryptographic algorithms employed by the certificate to protect its data, as per Claim 1.

Schneier appears to describe a standard X.509 certificate which employs a single cryptographic algorithm.

Including a list of cryptographic algorithms as data in a certificate does not teach, suggest or disclose using multiple algorithms to protect the data in the certificate. There is no reason to combine Shambroom's list of cryptographic algorithms contained in a certificate (which indicate which algorithms a server supports) with the standard

X.509 certificate, such as that of Schneier, which actually uses a single algorithm to protect data contained therein.

The final Office Action also uses the Shear reference in combination with Shambroom and Schneier to reject Claim 1. Shear is directed to security for load modules. In the Abstract, Shear states that the use of "several dissimilar digital signature algorithms may be used to reduce vulnerability from algorithm compromise, and subsets of multiple digital signatures may be used to reduce the scope of any specific compromise."

However, Shear does not suggest, teach or disclose creating extensions to a certificate. The Office Action argues that it would be obvious to put multiple signatures formed with different algorithms into Shambroom's certificate based on the teachings of Shear.

Applicant has never argued that the present invention claims the concept of using more than one algorithm for the purpose of security. Rather, Applicant has figured out how to make such a multiple algorithm system work with respect to certificates. This involves the use of extensions. And none of the references teaches this or mentions the use of extensions in such a manner. None of Shambroom, Shear and Schneier discusses the use of extensions to enable the certificate to support an alternative cryptographic algorithm, as per the second and third elements of Claim 1.

In a number of the Office Actions, the Examiner has noted that "one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references." On some level, this may be true. However, if an applicant can show that a given reference does not in fact teach, suggest or disclose those portions of the claims that the reference is utilized in a rejection to teach, suggest or disclose, then the combination is improper and the obviousness rejection cannot stand. If individual references may not be attacked, then a reference directed to mousetraps

could be combined with a reference directed to a semiconductor in order to render claims directed to bioengineered corn obvious with neither the semiconductor reference nor the mousetrap reference being 'attackable' individually. Certainly, each reference may be 'attacked' for not teaching, suggesting or disclosing what they are alleged to teach, suggest or show, thus rendering the scope of the combination incomplete relative to the claimed subject matter.

In one of the Office Actions it is argued that "the bits in Shambroom that identify the cryptographic algorithms, which are additional information, read on an extension." What this discussion shows is that the rejections over the art are taking little bits and pieces out of the various cited references and combining them in a way not contemplated by the references as a collection and without an teaching to combine the references in the manner combined. Are "bits" from Shambroom to which the Office Action is referring to the "list" of algorithms. An extension is a well-defined term of art in the certificate art. The addition of bits to a list of algorithms does not teach, suggest or disclose adding an extension to a certificate.

In the Office Action dated April 15, 2003, it was argued in numbered paragraph 3 that the fact that the "present invention does not transfer data that includes a list of cryptographic algorithms" does not matter, because "applicant has recognized another advantage which would flow naturally from following the suggestion of the prior art..." Applicant has made no such recognition. As discussed above, a list of algorithms does not anticipates an extension for identifying at least one alternative algorithm. The argument in paragraph 3 is not supported by Shambroom. Shambroom does not mention certificate extensions. The Shambroom list is not a certificate extension. There is no mention that the list takes the form of a certificate extension. Rather, as discussed above, the list is data which is relevant to which algorithms the network server supports. They have nothing to do with protecting the information in the certificate, as per the claimed subject matter.

In numbered paragraph six of the April 15, 2003 Office Action, the Office Action states that the combination of references is proper because "Shear et al, while specifically directed to load modules, executables, and other data elements teaches multiple signatures created with dissimilar algorithms in a broadly applicable fashion, and thus the combination is proper." As noted above, the most pertinent passage of Shear states, in the Abstract, that the use of "several dissimilar digital signature algorithms may be used to reduce vulnerability from algorithm compromise, and subsets of multiple digital signatures may be used to reduce the scope of any specific compromise." Shear is directed to security for load modules. There is nothing in the art that suggests the desirability to combine the references. Shear is directed to load modules and executables, not certificates. The ability to enable a certificate to support more than one cryptographic algorithm is an entirely different problem.

In numbered paragraph seven of the Office Action of April 15, 2003, the Office Action erroneously states that "applicant agrees that the claims recite data." What Applicant stated is that the claims recite functional structure for data, much like Shear. It is interesting that the Office Action goes on to state that Shear claims physical objects. If this is the case, then Shear clearly cannot be combined with the other references, as the other references are not directed to physical objects. However, Applicant believes Shear to be directed to code, and the barrier, arrangement and load module of Shear's claim 14 are certainly not a physical barrier, a physical arrangement and a physical load module, but functional structures for data. Physical names have been provided to these structural elements which are purely code based.

Accordingly, Applicant submits that Claim 1 patentably distinguishes over the combination of Shambroom, Shear and Schneier. Applicant respectfully request that the Board overturn this rejection of Claim 1

2. Independent Claims 4, 7 and 10

Independent Claims 4, 7 and 10 were rejected for the same reasons as was independent Claim 1. Accordingly, it follows that Claims 4, 7 and 10 distinguish over the cited art, and respectfully request that the Board overturn these rejections.

3. Dependent Claims 2, 3, 5, 6, 8, 9, 11 and 12

Since the independent claims have been shown to patentably distinguish over the cited art, it follows that the dependent claims also distinguish therefrom. Accordingly, Applicant respectfully requests that the Board overturn the rejection of Claim 2, 3, 5, 6, 8, 9, 11 and 12 over the art.

B. Improper Combination of References

Additionally, the Examiner has failed to provide a convincing line of reasoning for combining the teachings and structure of Shambroom with the teachings and structure of Schneier and the teachings and structure of Shear so as to arrive at the present claimed invention. Under 35 U.S.C. Section 103, when the Examiner has relied on the teachings of several references, the test is whether or not the references viewed individually and collectively would have suggested the claimed invention to the person possessing ordinary skill in the art. See *In re Kaslow*, 707 F.2d 1366, 217 USPQ 1989 (Fed. Cir. 1983). It is to be noted, however, that citing references which merely indicate that isolated elements and/or features recited in the claims are known is not a sufficient basis for concluding that a combination of claimed elements would have been obvious. That is to say, there should be something in the prior art or a convincing line of reasoning suggesting the desirability of combining the references in such a manner as to arrive at the claimed invention. See *In re Deminski*, 796 F.2d 436, 230 USPQ 313 (Fed. Cir. 1986).

Applicant submits that there is no teaching in the reference or a convincing line

of reasoning provided by the Examiner to combine the teachings of Shambroom, Shear and Schneier so as to arrive at the present claimed invention. Shambroom discloses a certificate that contains a list of one or more cryptographic algorithms that a **network server** support. Schneier describes a standard X.509 certificate which employs a single cryptographic algorithm. Shear is directed to security for load modules which uses several dissimilar digital signature algorithms. No reason is provided for combining a certificate which carries a list of algorithms (Shambroom) with a standard X.509 certificate (Schneier) with the concept that multiple dissimilar digital signature algorithms may be used for security for load modules. How and why anyone would combine these references so as to arrive at the present claimed invention is entirely unclear. Certainly, nothing is provided in the references that would suggest combining these references. No appropriate line of reasoning is provided for combining these references. Accordingly, Applicant submits that the combination of references is inappropriate and improper and respectfully submit that this is a further reason to overturn the rejection that stands alone from the reasons discussed above relative to the content of the references.

Accordingly, Applicant submits that Claims 1-12 further distinguish over the cited art, and respectfully request that the Board overturn the rejection over the art for this reason as well.

C. Traversal of the Rejection under 35 U.S.C. Section 101

Claims 1 - 3 were rejected under 35 U.S.C. Section 101 for being directed to non-statutory subject matter. The rejection states that the claims "claim data."

Applicant submits that the claims are statutory. The claims recite a functional structure for data stored on a computer readable media. The claims do not recite sales data or a list of addresses. For example, in the Shear patent cited by the Examiner, Claims 14 and 34 recite a security structure. The barrier, arrangement and load

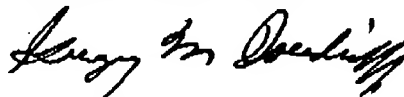
module of Shear's claim 14 are certainly not a physical barrier, a physical arrangement and a physical load module, but functional structures for data. This claim format is well accepted by the United States Patent and Trademark Office as being appropriate. The Office Actions do not describe in any detail why the claims of the present invention are unpatentable while the claims of Shear are patentable. The Office Actions have no detailed discussion as to why the claims are non-statutory. Since issued claims exist under the format alleged to be non-statutory in the final Office Action and no detailed explanation has been provided as to why the present claims are non-statutory while the issued claims are statutory, Applicant submits that this rejection is erroneous, and that Claims 1-3 are statutory. It also appears to follow that the USPTO is estopped from taking a different position relative to the present claims given its prior position on the same claim format without the benefit of any intervening statute or case law.

Accordingly, Applicant submits that Claims 1-3 are statutory, and respectfully requests that the Board overturn the rejection

SUMMARY

Applicant respectfully submits that the final rejections of the claims under 35 U.S.C. Sections 103(a) and 101 are improper and erroneous. Applicant respectfully urges the Board of Patent Appeals to reverse all grounds of the final rejection relative to the claims.

Respectfully submitted,



Gregory M. Doudnikoff
Attorney for Applicant
Reg. No. 32,847

GMD:ssc

Docket No: CR9-98-095
PHONE: 919-254-1288
FAX: 919-254-4330

Serial No. 09/240,265

12

APPENDIX

1. An X.509 certificate stored on computer readable medium, said certificate capable of supporting more than one cryptographic algorithm, comprising:

a signature algorithm and signature for all authenticated attributes using a first cryptographic algorithm;

an alternative public key extension for identifying at least one alternative cryptographic algorithm and providing its associated public key; and

an alternative signature extension for containing a signature for the alternative cryptographic algorithm.

2. An X.509 certificate according to Claim 1, wherein the first cryptographic algorithm is RSA and the alternative cryptographic algorithm is elliptic curve.

3. An X.509 certificate according to Claim 1, wherein the certificate can be verified by either the signature for the first cryptographic algorithm or the signature for the alternative signature algorithm.

4. A method for enabling an X.509 certificate to support more than one cryptographic algorithm, said method comprising the steps of:

providing the X.509 certificate with a signature algorithm and signature for all authenticated attributes using a first cryptographic algorithm;

providing the X.509 certificate with an alternative public key extension for identifying at least one alternative cryptographic algorithm and providing its associated public key; and

providing the X.509 certificate with an alternative signature extension which contains a signature for the alternative cryptographic algorithm.

5. A method for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 4, wherein the first cryptographic algorithm is RSA and the alternative cryptographic algorithm is elliptic curve.

6. A method for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 4, wherein the certificate can be verified by either the signature for the first cryptographic algorithm or the signature for the alternative signature algorithm.

7. Computer readable code stored on computer readable media for enabling an X.509 certificate to support more than one cryptographic algorithm, said computer readable code comprising:

first subprocesses for providing the X.509 certificate with a signature algorithm and signature for all authenticated attributes using a first cryptographic algorithm;

second subprocesses for providing the X.509 certificate with an alternative public key extension for identifying at least one alternative cryptographic algorithm and providing its associated public key; and

third subprocesses for providing the X.509 certificate with an alternative signature extension which contains a signature for the alternative cryptographic algorithm.

8. Computer readable code for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 7, wherein the first cryptographic algorithm is RSA and the alternative cryptographic algorithm is elliptic curve.

9. Computer readable code for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 7, wherein the certificate can be verified by either the signature for the first cryptographic algorithm or the signature for the alternative signature algorithm.

10. In a computing environment, a system for enabling an X.509 certificate to support more than one cryptographic algorithm, said system comprising:

means for providing the X.509 certificate with a signature algorithm and signature for all authenticated attributes using a first cryptographic algorithm;

means for providing the X.509 certificate with an alternative public key extension for identifying at least one alternative cryptographic algorithm and providing its associated public key; and

means for providing the X.509 certificate with an alternative signature extension which contains a signature for the alternative cryptographic algorithm.

11. A system for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 10, wherein the first cryptographic algorithm is RSA and the alternative cryptographic algorithm is elliptic curve.

12. A system for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 10, wherein the certificate can be verified by either the signature for the first cryptographic algorithm or the signature for the alternative signature algorithm.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of : December 20, 2004
Mark E. Peters : IBM Corporation
Ser. No. 09/240,265 : Dept.T81/Bldg. 503
Filed January 29, 1999 : P.O. Box 12195
For: Extension of X.509 Certificates to : Res. Tri. Park, NC 27709
Simultaneously Support Multiple : Art Unit: 2137
Cryptographic Algorithms : Examiner: D. J. Meislahn

APPEAL BRIEF

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Sir:

The following remarks in the Appeal for the above identified Application are respectfully submitted:

REAL PARTY IN INTEREST

This Application has been assigned to the International Business Machines Corporation.

RELATED APPEALS AND INTERFERENCES

Applicants know of no other Appeals or Interferences which will directly affect or

Serial No. 09/240,265

1

be directly affected by or having a bearing on the Boards decision in the pending Appeal.

STATUS OF CLAIMS

The Application was originally filed with Claims 1 - 3. Claims 4 - 6 were added in the Amendment filed on February 12, 2003. Claims 5 and 6 were amended and Claims 7 - 9 were added in the Amendment filed on July 15, 2003. Claims 1 and 7 were amended and Claims 10 - 12 were added in the Amendment dated February 9, 2004. Accordingly, Claims 1 - 12 remain pending, and these are the claims which are the subject of this Appeal. A copy of the appealed claims, Claims 1 - 12, are contained in the attached Appendix.

STATUS OF AMENDMENTS

Applicants last filed an Amendment on February 9, 2004, which was entered. No further amendments were made to the Application.

SUMMARY OF THE INVENTION

The present invention discloses an extended X.509 certificate capable of supporting more than one cryptographic algorithm. The certificate comprises a signature algorithm and a signature for all authenticated attributes using a first cryptographic algorithm, and alternative public key extension for identifying at least one alternative cryptographic algorithm and providing its associated public key, and an alternative signature extension for containing a signature for the alternative cryptographic algorithm.

STATEMENT OF ISSUES PRESENTED

Applicants present for review the final rejection of Claims 1 through 12 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,923,756 to Shambroom and passages from the Schneier book "Applied Cryptography" in view of U.S. Patent No. 6,157,721 to Shear et al. Applicants also present for review the final rejection of Claims 1 - 3 under 35 U.S.C. Section 101 for being directed to non-statutory subject matter.

GROUPING OF THE CLAIMS

Independent Claim 1 stands or falls alone.

Dependent Claims 2 and 3 stand or fall with Claim 1.

Independent Claims 4, 7 and 10 stand or fall together.

Dependent Claims 5, 6, 8, 9, 11 and 12 stand or fall with Claims 4, 7 and 10.

ARGUMENT

Applicant traverses the rejections below.

A. Differences Between the Claimed Invention and the Cited Art

1. Independent Claim 1

Claims 1 through 12 were rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,923,756 to Shambroom and passages from the Schneier book "Applied Cryptography" in view of U.S. Patent No. 6,157,721 to Shear et al.

Shambroom discloses a technique for enhancing the security of a message sent through a network server from a client computer to a destination server. A secure connection for receiving and transmitting data is established between the client and the server. Using client identification information and a secure authentication protocol, the server obtains client-authentication information from a validation center. This information is transmitted to the client and erased from the server.

Relative to Claim 1, the Office Action identifies a passage from Shambroom as disclosing "a certificate that supports one or more cryptographic algorithms" and that "the certificate can resemble an X.509 certificate," citing Column 10, lines 32-35

More specifically, Shambroom states that "web server 720 responds with a certificate to web browser 620. This certificate contains the network server's public key and a list of one or more cryptographic algorithms that the network server supports..." (Column 10, lines 30-34).

The key here is that the Shambroom certificate contains a **list** of one or more cryptographic algorithms that the **network server** supports. The Shambroom certificate does not actually use or employ multiple cryptographic algorithms to protect the data therein. The Shambroom data appears to be the list of algorithms. The certificate in Claim 1 does **not** contain a list of cryptographic algorithms that a network server supports. The claimed certificate utilizes and uses more than one cryptographic algorithm itself to protect the data it includes.

Further, the network server's public key appears to be used by the web browser to log onto or communicate with the web server 720, which is part of the network server 700, and not to protect the data in the certificate. In other words, the Shambroom certificate is used to transfer data, including the list of cryptographic algorithms that the network server supports and the public key for the network server, to the web browser.

No such scheme is contemplated by the present invention.

The Office Action goes on to state that the "list of algorithms disclosed in Shambroom also anticipates an extension for identifying at least one alternative algorithm." This statement is not supported by Shambroom. Shambroom does not mention certificate extensions. The Shambroom list is not a certificate extension. There is no mention that the list takes the form of a certificate extension. Rather, as discussed above, the list is data which is relevant to which algorithms the network server supports. They have nothing to do with protecting the information in the certificate, as per the claimed subject matter.

Claim 1 recites that the X.509 certificate comprises "a signature algorithm and signature for all authenticated attributes using a first cryptographic algorithm;" as well as "an alternative public key extension for identifying at least one alternative cryptographic algorithm and providing its associated public key; and an alternative signature extension for containing a signature for the alternative cryptographic algorithm." This is not the same thing as a list of cryptographic algorithms that a network server supports as per Shambroom, and such a list included in a certificate does not teach, suggest or disclose the subject matter of Claim 1. Shambroom does not teach that its certificate protects its data using more than one cryptographic algorithm. The Shambroom list appears to be data included in the certificate, not multiple cryptographic algorithms employed by the certificate to protect its data, as per Claim 1.

Schneier appears to describe a standard X.509 certificate which employs a single cryptographic algorithm.

Including a list of cryptographic algorithms as data in a certificate does not teach, suggest or disclose using multiple algorithms to protect the data in the certificate. There is no reason to combine Shambroom's list of cryptographic algorithms contained in a certificate (which indicate which algorithms a server supports) with the standard

X.509 certificate, such as that of Schneier, which actually uses a single algorithm to protect data contained therein.

The final Office Action also uses the Shear reference in combination with Shambroom and Schneier to reject Claim 1. Shear is directed to security for load modules. In the Abstract, Shear states that the use of "several dissimilar digital signature algorithms may be used to reduce vulnerability from algorithm compromise, and subsets of multiple digital signatures may be used to reduce the scope of any specific compromise."

However, Shear does not suggest, teach or disclose creating extensions to a certificate. The Office Action argues that it would be obvious to put multiple signatures formed with different algorithms into Shambroom's certificate based on the teachings of Shear.

Applicant has never argued that the present invention claims the concept of using more than one algorithm for the purpose of security. Rather, Applicant has figured out how to make such a multiple algorithm system work with respect to certificates. This involves the use of extensions. And none of the references teaches this or mentions the use of extensions in such a manner. None of Shambroom, Shear and Schneier discusses the use of extensions to enable the certificate to support an alternative cryptographic algorithm, as per the second and third elements of Claim 1.

In a number of the Office Actions, the Examiner has noted that "one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references." On some level, this may be true. However, if an applicant can show that a given reference does not in fact teach, suggest or disclose those portions of the claims that the reference is utilized in a rejection to teach, suggest or disclose, then the combination is improper and the obviousness rejection cannot stand. If individual references may not be attacked, then a reference directed to mousetraps

could be combined with a reference directed to a semiconductor in order to render claims directed to bioengineered corn obvious with neither the semiconductor reference nor the mousetrap reference being 'attackable' individually. Certainly, each reference may be 'attacked' for not teaching, suggesting or disclosing what they are alleged to teach, suggest or show, thus rendering the scope of the combination incomplete relative to the claimed subject matter.

In one of the Office Actions it is argued that "the bits in Shambroom that identify the cryptographic algorithms, which are additional information, read on an extension." What this discussion shows is that the rejections over the art are taking little bits and pieces out of the various cited references and combining them in a way not contemplated by the references as a collection and without an teaching to combine the references in the manner combined. Are "bits" from Shambroom to which the Office Action is referring to the "list" of algorithms. An extension is a well-defined term of art in the certificate art. The addition of bits to a list of algorithms does not teach, suggest or disclose adding an extension to a certificate.

In the Office Action dated April 15, 2003, it was argued in numbered paragraph 3 that the fact that the "present invention does not transfer data that includes a list of cryptographic algorithms" does not matter, because "applicant has recognized another advantage which would flow naturally from following the suggestion of the prior art..." Applicant has made no such recognition. As discussed above, a list of algorithms does not anticipate an extension for identifying at least one alternative algorithm. The argument in paragraph 3 is not supported by Shambroom. Shambroom does not mention certificate extensions. The Shambroom list is not a certificate extension. There is no mention that the list takes the form of a certificate extension. Rather, as discussed above, the list is data which is relevant to which algorithms the network server supports. They have nothing to do with protecting the information in the certificate, as per the claimed subject matter.

In numbered paragraph six of the April 15, 2003 Office Action, the Office Action states that the combination of references is proper because "Shear et al, while specifically directed to load modules, executables, and other data elements teaches multiple signatures created with dissimilar algorithms in a broadly applicable fashion, and thus the combination is proper." As noted above, the most pertinent passage of Shear states, in the Abstract, that the use of "several dissimilar digital signature algorithms may be used to reduce vulnerability from algorithm compromise, and subsets of multiple digital signatures may be used to reduce the scope of any specific compromise." Shear is directed to security for load modules. There is nothing in the art that suggests the desirability to combine the references. Shear is directed to load modules and executables, not certificates. The ability to enable a certificate to support more than one cryptographic algorithm is an entirely different problem.

In numbered paragraph seven of the Office Action of April 15, 2003, the Office Action erroneously states that "applicant agrees that the claims recite data." What Applicant stated is that the claims recite functional structure for data, much like Shear. It is interesting that the Office Action goes on to state that Shear claims physical objects. If this is the case, then Shear clearly cannot be combined with the other references, as the other references are not directed to physical objects. However, Applicant believes Shear to be directed to code, and the barrier, arrangement and load module of Shear's claim 14 are certainly not a physical barrier, a physical arrangement and a physical load module, but functional structures for data. Physical names have been provided to these structural elements which are purely code based.

Accordingly, Applicant submits that Claim 1 patentably distinguishes over the combination of Shambroom, Shear and Schneier. Applicant respectfully request that the Board overturn this rejection of Claim 1

2. Independent Claims 4, 7 and 10

Independent Claims 4, 7 and 10 were rejected for the same reasons as was independent Claim 1. Accordingly, it follows that Claims 4, 7 and 10 distinguish over the cited art, and respectfully request that the Board overturn these rejections.

3. Dependent Claims 2, 3, 5, 6, 8, 9, 11 and 12

Since the independent claims have been shown to patentably distinguish over the cited art, it follows that the dependent claims also distinguish therefrom. Accordingly, Applicant respectfully requests that the Board overturn the rejection of Claim 2, 3, 5, 6, 8, 9, 11 and 12 over the art.

B. Improper Combination of References

Additionally, the Examiner has failed to provide a convincing line of reasoning for combining the teachings and structure of Shambroom with the teachings and structure of Schneler and the teachings and structure of Shear so as to arrive at the present claimed invention. Under 35 U.S.C. Section 103, when the Examiner has relied on the teachings of several references, the test is whether or not the references viewed individually and collectively would have suggested the claimed invention to the person possessing ordinary skill in the art. See *In re Kaslow*, 707 F.2d 1366, 217 USPQ 1989 (Fed. Cir. 1983). It is to be noted, however, that citing references which merely indicate that isolated elements and/or features recited in the claims are known is not a sufficient basis for concluding that a combination of claimed elements would have been obvious. That is to say, there should be something in the prior art or a convincing line of reasoning suggesting the desirability of combining the references in such a manner as to arrive at the claimed invention. See *In re Deminski*, 796 F.2d 436, 230 USPQ 313 (Fed. Cir. 1986).

Applicant submits that there is no teaching in the reference or a convincing line

of reasoning provided by the Examiner to combine the teachings of Shambroom, Shear and Schneier so as to arrive at the present claimed invention. Shambroom discloses a certificate that contains a list of one or more cryptographic algorithms that a network server support. Schneier describes a standard X.509 certificate which employs a single cryptographic algorithm. Shear is directed to security for load modules which uses several dissimilar digital signature algorithms. No reason is provided for combining a certificate which carries a list of algorithms (Shambroom) with a standard X.509 certificate (Schneier) with the concept that multiple dissimilar digital signature algorithms may be used for security for load modules. How and why anyone would combine these references so as to arrive at the present claimed invention is entirely unclear. Certainly, nothing is provided in the references that would suggest combining these references. No appropriate line of reasoning is provided for combining these references. Accordingly, Applicant submits that the combination of references is inappropriate and improper and respectfully submit that this is a further reason to overturn the rejection that stands alone from the reasons discussed above relative to the content of the references.

Accordingly, Applicant submits that Claims 1-12 further distinguish over the cited art, and respectfully request that the Board overturn the rejection over the art for this reason as well.

C. Traversal of the Rejection under 35 U.S.C. Section 101

Claims 1 - 3 were rejected under 35 U.S.C. Section 101 for being directed to non-statutory subject matter. The rejection states that the claims "claim data."

Applicant submits that the claims are statutory. The claims recite a functional structure for data stored on a computer readable media. The claims do not recite sales data or a list of addresses. For example, in the Shear patent cited by the Examiner, Claims 14 and 34 recite a security structure. The barrier, arrangement and load

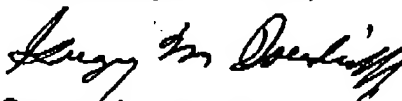
module of Shear's claim 14 are certainly not a physical barrier, a physical arrangement and a physical load module, but functional structures for data. This claim format is well accepted by the United States Patent and Trademark Office as being appropriate. The Office Actions do not describe in any detail why the claims of the present invention are unpatentable while the claims of Shear are patentable. The Office Actions have no detailed discussion as to why the claims are non-statutory. Since issued claims exist under the format alleged to be non-statutory in the final Office Action and no detailed explanation has been provided as to why the present claims are non-statutory while the issued claims are statutory, Applicant submits that this rejection is erroneous, and that Claims 1-3 are statutory. It also appears to follow that the USPTO is estopped from taking a different position relative to the present claims given its prior position on the same claim format without the benefit of any intervening statute or case law.

Accordingly, Applicant submits that Claims 1-3 are statutory, and respectfully requests that the Board overturn the rejection

SUMMARY

Applicant respectfully submits that the final rejections of the claims under 35 U.S.C. Sections 103(a) and 101 are improper and erroneous. Applicant respectfully urges the Board of Patent Appeals to reverse all grounds of the final rejection relative to the claims.

Respectfully submitted,



Gregory M. Doudnikoff
Attorney for Applicant
Reg. No. 32,847

2004-12-20 15:52

919-254-4330

919-254-4330 >> USPTO

P 52/55

GMD:ssc

Docket No: CR9-98-095

PHONE: 919-254-1288

FAX: 919-254-4330

Serial No. 09/240,265

12

APPENDIX

1. An X.509 certificate stored on computer readable medium, said certificate capable of supporting more than one cryptographic algorithm, comprising:

a signature algorithm and signature for all authenticated attributes using a first cryptographic algorithm;

an alternative public key extension for identifying at least one alternative cryptographic algorithm and providing its associated public key; and

an alternative signature extension for containing a signature for the alternative cryptographic algorithm.

2. An X.509 certificate according to Claim 1, wherein the first cryptographic algorithm is RSA and the alternative cryptographic algorithm is elliptic curve.

3. An X.509 certificate according to Claim 1, wherein the certificate can be verified by either the signature for the first cryptographic algorithm or the signature for the alternative signature algorithm.

4. A method for enabling an X.509 certificate to support more than one cryptographic algorithm, said method comprising the steps of:

providing the X.509 certificate with a signature algorithm and signature for all authenticated attributes using a first cryptographic algorithm;

providing the X.509 certificate with an alternative public key extension for identifying at least one alternative cryptographic algorithm and providing its associated public key; and

providing the X.509 certificate with an alternative signature extension which contains a signature for the alternative cryptographic algorithm.

5. A method for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 4, wherein the first cryptographic algorithm is RSA and the alternative cryptographic algorithm is elliptic curve.

6. A method for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 4, wherein the certificate can be verified by either the signature for the first cryptographic algorithm or the signature for the alternative signature algorithm.

7. Computer readable code stored on computer readable media for enabling an X.509 certificate to support more than one cryptographic algorithm, said computer readable code comprising:

first subprocesses for providing the X.509 certificate with a signature algorithm and signature for all authenticated attributes using a first cryptographic algorithm;

second subprocesses for providing the X.509 certificate with an alternative public key extension for identifying at least one alternative cryptographic algorithm and providing its associated public key; and

third subprocesses for providing the X.509 certificate with an alternative signature extension which contains a signature for the alternative cryptographic algorithm.

8. Computer readable code for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 7, wherein the first cryptographic algorithm is RSA and the alternative cryptographic algorithm is elliptic curve.

9. Computer readable code for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 7, wherein the certificate can be verified by either the signature for the first cryptographic algorithm or the signature for the alternative signature algorithm.

10. In a computing environment, a system for enabling an X.509 certificate to support more than one cryptographic algorithm, said system comprising:

means for providing the X.509 certificate with a signature algorithm and signature for all authenticated attributes using a first cryptographic algorithm;

means for providing the X.509 certificate with an alternative public key extension for identifying at least one alternative cryptographic algorithm and providing its associated public key; and

means for providing the X.509 certificate with an alternative signature extension which contains a signature for the alternative cryptographic algorithm.

11. A system for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 10, wherein the first cryptographic algorithm is RSA and the alternative cryptographic algorithm is elliptic curve.

12. A system for enabling an X.509 certificate to support more than one cryptographic algorithm according to Claim 10, wherein the certificate can be verified by either the signature for the first cryptographic algorithm or the signature for the alternative signature algorithm.